Managing A Multi-site Distributed Deployment Without Going Insane

Kevin Donahoe

Principal Engineer, AT&T Entertainment Group

.conf2016

splunk>

Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not, be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

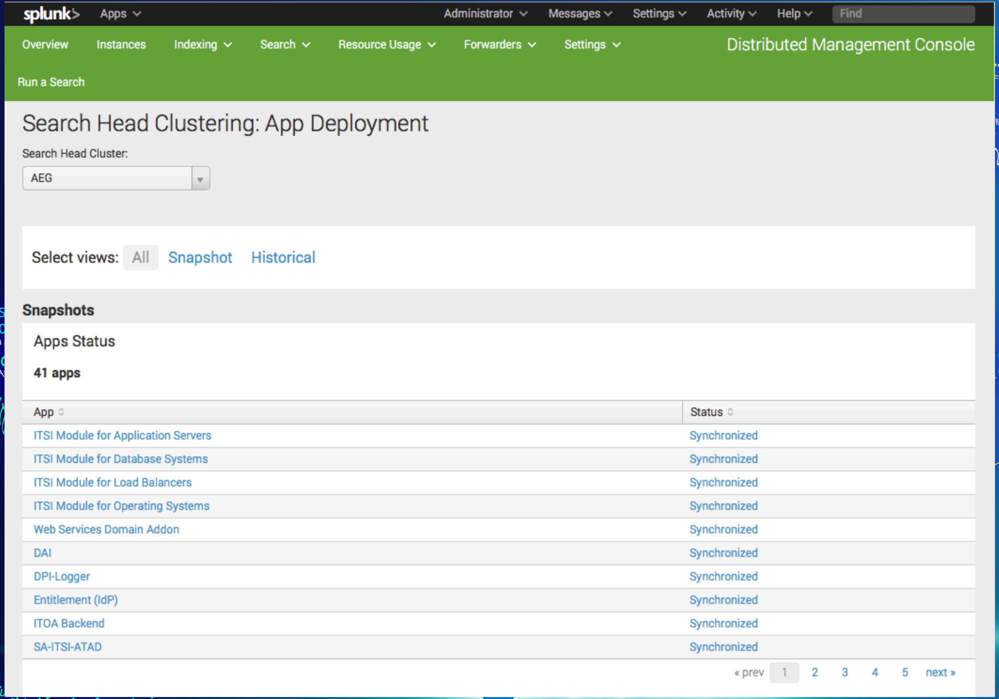
Agenda

- The challenge of a distributed, clustered environment:
  - Index clusters are very different than search head clusters
    - Requires different change management approaches
      - Indexer changes often require rolling restart which incurs replication activity
      - Search head changes are usually minor changes with minimal impact
- The solution: One Strategy to Rule Them All
  - A single source of truth. i.e. source control
  - Process Automation
- The Process:
  - Change Management & Control Strategy

The Challenge

Different Cluster Behavior

- Search head clusters config bundles move all local configs to default path and are overridden by web UI changes.
- This means the config bundle may not be the source of truth.
- Configuration changes are usually low impact.
- Configuration changes happen quite often.



Search Head Clustering: App Deployment

Search Head Cluster: AEG

Select views: All Snapshot Historical

Snapshots

Apps Status

41 apps

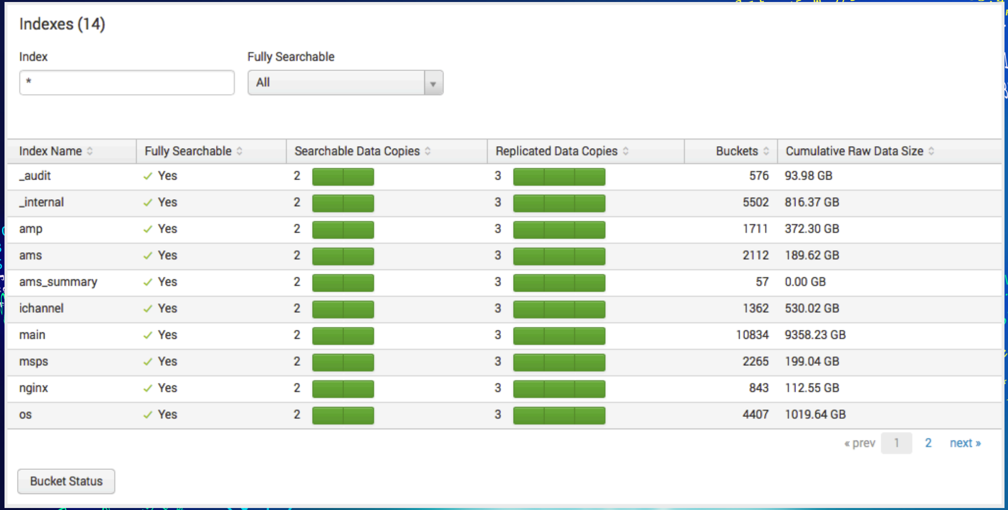
App	Status
ITSI Module for Application Servers	Synchronized
ITSI Module for Database Systems	Synchronized
ITSI Module for Load Balancers	Synchronized
ITSI Module for Operating Systems	Synchronized
Web Services Domain Addon	Synchronized
DAI	Synchronized
DPI-Logger	Synchronized
Entitlement (IdP)	Synchronized
ITOA Backend	Synchronized
SA-ITSI-ATAD	Synchronized

splunk>

The Challenge

Different Cluster Behavior

- Index clusters can experience performance impact from replication activity caused by a rolling restart.
- Configuration changes are usually higher impact.
- Configuration changes happen less often.



Indexes (14)

Index: *

Fully Searchable: All

Index Name	Fully Searchable	Searchable Data Copies	Replicated Data Copies	Buckets	Cumulative Raw Data Size
_audit	✓ Yes	2 🟩	3 🟩	576	93.98 GB
_internal	✓ Yes	2 🟩	3 🟩	5502	816.37 GB
amp	✓ Yes	2 🟩	3 🟩	1711	372.30 GB
ams	✓ Yes	2 🟩	3 🟩	2112	189.62 GB
ams_summary	✓ Yes	2 🟩	3 🟩	57	0.00 GB
ichannel	✓ Yes	2 🟩	3 🟩	1362	530.02 GB
main	✓ Yes	2 🟩	3 🟩	10834	9358.23 GB
msps	✓ Yes	2 🟩	3 🟩	2265	199.04 GB
nginx	✓ Yes	2 🟩	3 🟩	843	112.55 GB
os	✓ Yes	2 🟩	3 🟩	4407	1019.64 GB

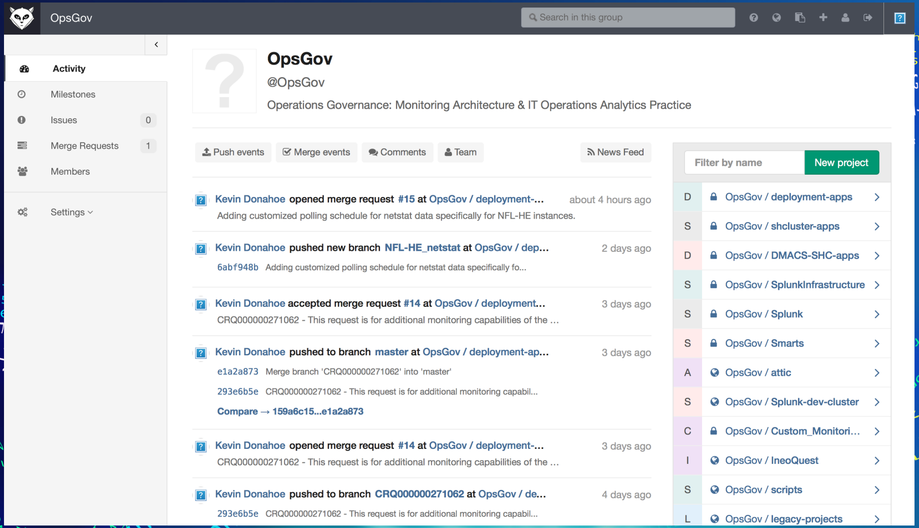
.conf2016

splunk>

The Solution

Source Control

- Source control provides a single source of truth with control over changes.
- Source control provides a roll-back method that is simple.
- Several open source solutions are available.



OpsGov

@OpsGov

Operations Governance: Monitoring Architecture & IT Operations Analytics Practice

Kevin Donahoe opened merge request #15 at OpsGov / deployment-... about 4 hours ago
Adding customized polling schedule for netstat data specifically for NFL-HE instances.

Kevin Donahoe pushed new branch NFL-HE_netstat at OpsGov / dep... 2 days ago
6abf948b Adding customized polling schedule for netstat data specifically fo...

Kevin Donahoe accepted merge request #14 at OpsGov / deployment... 3 days ago
CRQ000000271062 - This request is for additional monitoring capabilities of the …

Kevin Donahoe pushed to branch master at OpsGov / deployment-ap... 3 days ago
e1a2a873 Merge branch 'CRQ000000271062' into 'master'
293e6b5e CRQ000000271062 - This request is for additional monitoring capabil...
Compare → 159a6c15...e1a2a873

Kevin Donahoe opened merge request #14 at OpsGov / deployment-... 3 days ago
CRQ000000271062 - This request is for additional monitoring capabilities of the …

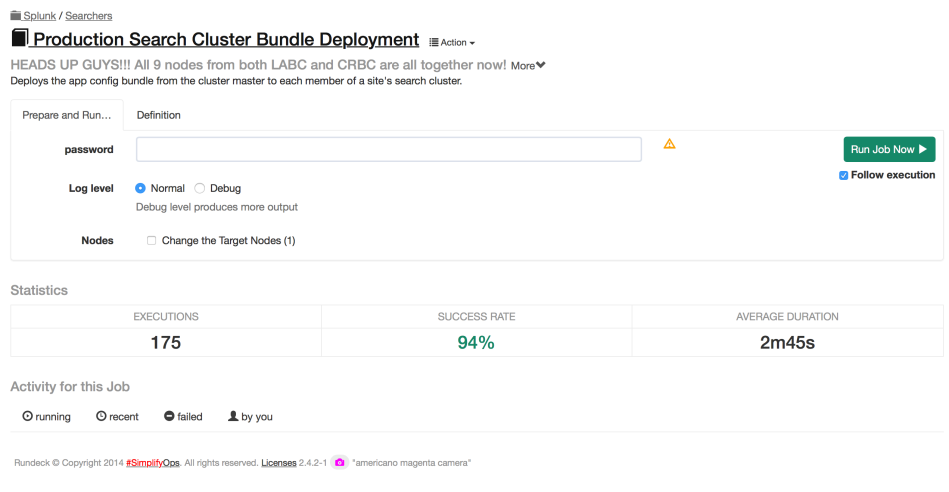
Kevin Donahoe pushed to branch CRQ000000271062 at OpsGov / de... 4 days ago
293e6b5e CRQ000000271062 - This request is for additional monitoring capabil...

D	OpsGov / deployment-apps
S	OpsGov / shcluster-apps
D	OpsGov / DMACS-SHC-apps
S	OpsGov / SplunkInfrastructure
S	OpsGov / Splunk
S	OpsGov / Smarts
A	OpsGov / attic
S	OpsGov / Splunk-dev-cluster
C	OpsGov / Custom_Monitori…
I	OpsGov / IneoQuest
S	OpsGov / scripts
L	OpsGov / legacy-projects

The Solution

Process Automation

- Process automation provides a common method of handling different repeatable processes.
- Process automation provides consistent process execution.



Splunk / Searchers

Production Search Cluster Bundle Deployment

HEADS UP GUYS!!! All 9 nodes from both LABC and CRBC are all together now! More

Deploys the app config bundle from the cluster master to each member of a site's search cluster.

☑ Follow execution

password

Log level ● Normal ○ Debug

Debug level produces more output

Nodes □ Change the Target Nodes (1)

Statistics

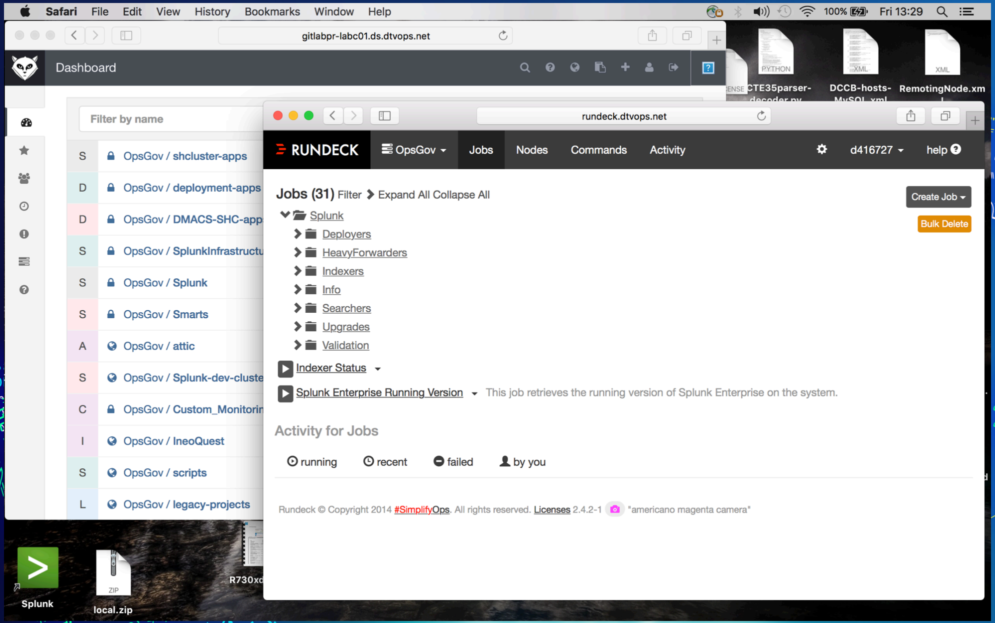
EXECUTIONS	SUCCESS RATE	AVERAGE DURATION
175	94%	2m45s

Activity for this Job

The Process

Change Management

- Usually a ticket system like Jira.
- Makes use of checks and balances to limit mistakes.
- Includes automatic testing to validate changes are benign.
- Requires a written Method of Procedure validated by peer review.
- Involves copious communication with stakeholders



S OpsGov / shcluster-apps
D OpsGov / deployment-apps
D OpsGov / DMACS-SHC-app
S OpsGov / SplunkInfrastructu
S OpsGov / Splunk
S OpsGov / Smarts
A OpsGov / attic
S OpsGov / Splunk-dev-cluste
C OpsGov / Custom_Monitorin
I OpsGov / IneoQuest
S OpsGov / scripts
L OpsGov / legacy-projects

Jobs (31) Filter > Expand All Collapse All

- Splunk
  - Deployers
  - HeavyForwarders
  - Indexers
  - Info
  - Searchers
  - Upgrades
  - Validation

Indexer Status

Splunk Enterprise Running Version — This job retrieves the running version of Splunk Enterprise on the system.

Activity for Jobs

running recent failed by you

Rundeck © Copyright 2014 #SimplifyOps. All rights reserved. Licenses 2.4.2-1 "americano magenta camera"

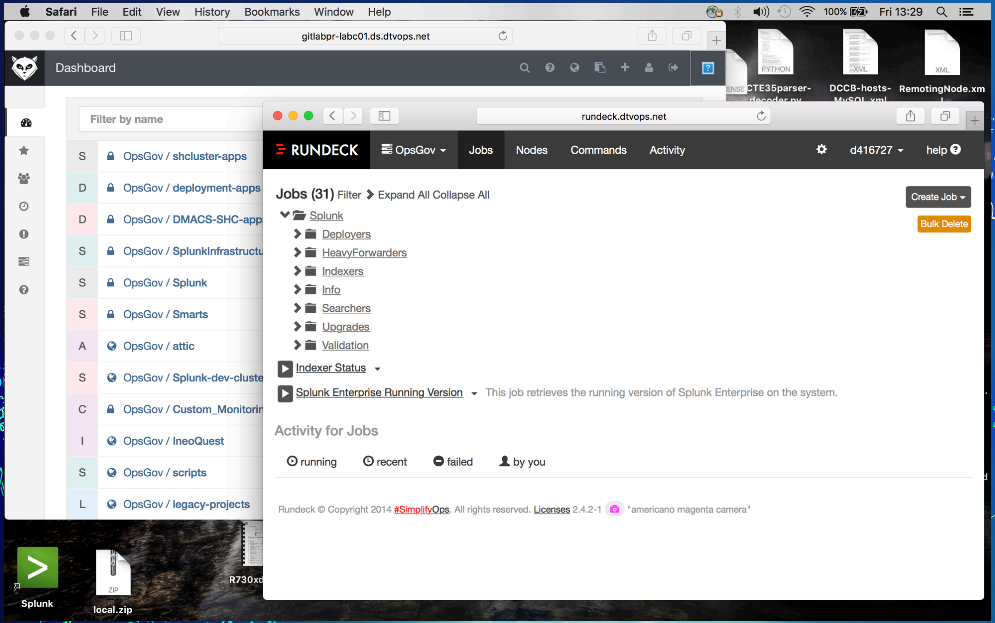
.conf2016

splunk>

The Process

Change Control

- Process automation provides consistent process execution.
- Empowers front line teams to execute without needing expertise in Splunk.
- Limits an operator to only the actions required to complete the change.
- Includes a full audit log of runs by operator to correlate with the change ticket.



S	OpsGov / shcluster-apps
D	OpsGov / deployment-apps
D	OpsGov / DMACS-SHC-app
S	OpsGov / SplunkInfrastructu
S	OpsGov / Splunk
S	OpsGov / Smarts
A	OpsGov / attic
S	OpsGov / Splunk-dev-cluste
C	OpsGov / Custom_Monitorin
I	OpsGov / IneoQuest
S	OpsGov / scripts
L	OpsGov / legacy-projects

Jobs (31) Filter Expand All Collapse All

- Splunk
  - Deployers
  - HeavyForwarders
  - Indexers
  - Info
  - Searchers
  - Upgrades
  - Validation
- Indexer Status
- Splunk Enterprise Running Version — This job retrieves the running version of Splunk Enterprise on the system.

Activity for Jobs

running recent failed by you

Rundeck © Copyright 2014 #SimplifyOps. All rights reserved. Licenses 2.4.2-1 "americano magenta camera"

THANK YOU

.conf2016

splunk>